Tecnologias de Redes de Comunicações

2006/2007

O protocolo RADIUS

Fernando M. Silva

Fernando.Silva@lx.it.pt

Instituto Superior Técnico

Sumário

- Introdução
- Sistemas AAA
- Protocolo Radius
- Autenticação
- *Accounting*
- Atributos
- Proxy radius
- Funcionamento

Autenticação local vs. autenticação centralizada

- O controlo de acesso a recursos informáticos é habitualmente realizado por um processo de autenticação, em que são verificadas as credenciais de acesso, dos quais o acesso por *username/password* é o mais generalizado
- Outros sistemas de autenticação, nomeadamente os baseados em chaves privadas, são mais seguros mas apresentam requisitos de utilização mais complexos
- Originalmente, as credenciais de acesso (em texto original ou cifradas) estavam simplesmente depositadas num ficheiro local na máquina de acesso.
- Com a multiplicação de diferentes pontos de acesso a recursos por parte de um mesmo utilizador, a replicação dos ficheiros de credenciais pelas diversas máquinas tornava-se inviável
- O protocolo RADIUS surgiu pela necessidade de construir uma infra-estrutura centralizada de autenticação, adequada a ambientes de acesso distribuídos, separando os recursos da fase de autenticação

Caracteristicas dos sistemas RADIUS

- Modelo cliente / servidor
- Possibilidade de operação em modo proxy, permitindo construir uma hierarquia de autenticação.
- Suporte de diferentes tipos de autenticação
- As mensagens são constituídas por atributos, comprimento e valor, permitindo assim a extensão do protocolo com novos atributos.

Sistemas AAA

O protocolo RADIUS tem não apenas o objectivo de autenticação, mas constitui um sistema completo de AAA - *Authentication, Authorization and Accounting*

- Autenticação: Garantia de identidade do utilizador
- Autorização: Permissão de acesso aos recursos disponíveis
- Accountig: Registo de sessões e contabilização de tráfego

Princípio de funcionamento

- O cliente obtem as credenciais do utilizador
- O cliente cria uma trama "Access-Request" que inclui as credenciais, e a identificação do porto/serviço de acesso.
  - Se não houver resposta num dado periodo de tempo, a trama é enviada novamente.
- O servidor RADIUS recebe o pedido e verifica as credenciais do utilizador e, opcionalmente, pode consultar uma base de dados de permissões para verificar se o utilizador tem permissão para aceder ao recurso.
  - O servidor pode consultar outros servidores, funcionando neste caso como cliente. Este é o modelo normalmente designado por *proxy-radius*.
  - O servidor pode responder de três formas:
    * Access-Reject
    * Access-Accept
    * Access-Challenge
      O servidor envia um desafio adicional ao cliente para autenticação.

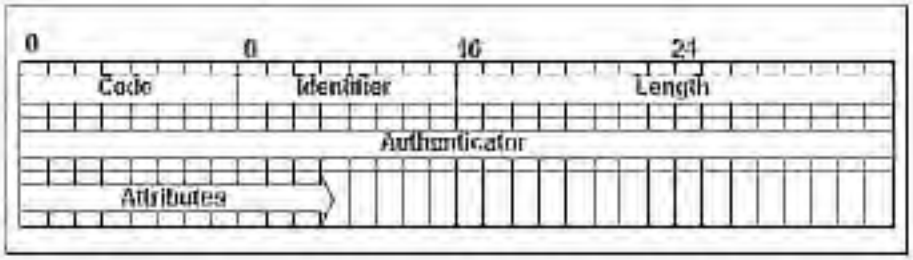
Transporte: UDP

- Justificação (original...)
  - Originalmente desenhado para meios com poucos erros
  - Maior fluidez de mensagens
  - Selecção mais rápida de um servidor alternativo
  - Handshaking incluido no protocolo
  - Maior facilidade de suportar solicitações múltiplas no servidor de autenticação (threads independentes).

UDP, mas...

- Visão actual
  - A utilização de RADIUS em meios sem fios, onde as perdas de pacotes são maiores, questionam a aproximação UDP.
  - A utilização de UDP em hierarquias de autenticação mais complexas conduz também a mais problemas, devido à possibilidade de ausência de respostas de servidores intermédios.
  - O maior débito das ligações e as facilidades de software existentes mitigam muitos dos argumentos originais a favor do RADIUS.
  - Recentemente (Junho de 2007), foi proposto um draft no IETF o protocolo RADSEC, que propõe o envio do *payload* RADIUS sobre uma ligação TCP+TLS, de modo a garantir um transporte seguro e sobre uma camada de transporte mais fiável.

Formato das tramas RADIUS



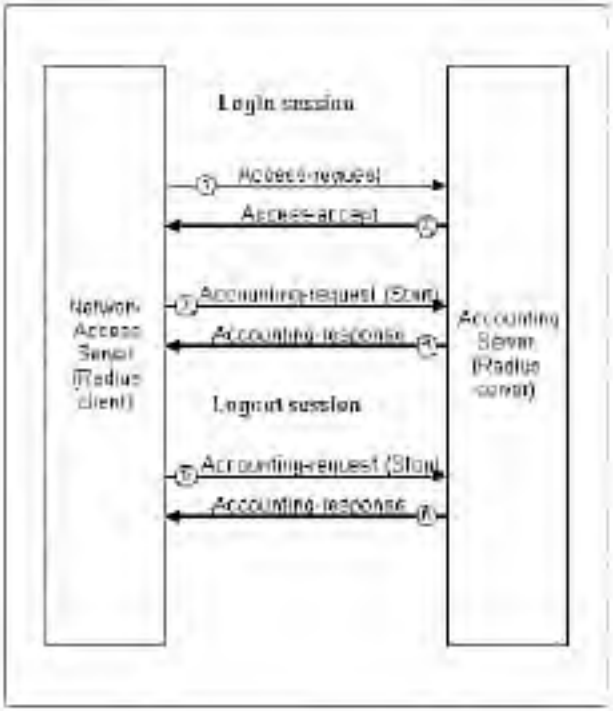
- Code - Um octeto com o código comando/resposta do RADIUS
  - access-request, (cliente →servidor). Pedido de acesso. Respostas possíveis:
    - * access-accept, (servidor →cliente) OK
    - * access-reject (servidor →cliente) Rejeição
    - * access-challenge, (servidor →cliente), resposta em que o servidor espera uma resposta do cliente encapsulada num acesso-request
    - * accounting request, (client-¿server), accounting response (servidor-¿cliente)
  - Identifier - Associação entre pedidos e respostas
  - Comprimento do campo (2 octetos)
  - Authenticator - Valor usado para autenticar a resposta e usado igualmente no algoritmos de verificação das credenciais.
  - Attributos - Os dados do comando ou resposta.

- Na sua forma mais simples, o RADIUS pode usar uma base de dados local de utilizadores e credenciais para verificação da identidade.
- Hoje em dia, a componente de autenticação de RADIUS é frequentemente delegada num sistema mais abrangente de autenticação
  - LDAP (Light Weight Directory Protocol)
    - Sistema de directório em que são registados vários atributos do utilizador (desde o nome, número de aluno, e-mail, morada, telefone), e em que o acesso a estes atributos é regulado por políticas de acesso.
  - Kerberos
    - Autenticação forte
  - LDAP+Kerberos
    - Sistema de autenticação baseado em LDAP mas em que este delega, por sua vez, a autenticação num sistema Kerberos.
  - Apesar da existência de outros sistemas de autenticação, o RADIUS é frequentemente usado pelo suporte nativo que tem de registos de *accounting*.

Accounting

- O sistema de *accounting* do RADIUS permite o controlo e registo detalhado da utilização dos recursos de rede por parte dos clientes, sendo por isso o modo preferido de contabilização e registo de recursos por parte dos operadores.
- No início da sessão, e após a autenticação, o cliente envia para o servidor uma mensagem de Accounting-Request, com opção START.
  - Ao receber esta msg, o servidor regista o utilizador, a data/hora de inicio de sessão, e alguns parâmetros adicionais que tenham sido enviados pelo cliente.
  - O servidor deve responder a este pedido com uma mensagem *Accounting-Response*
- No final da sessão, o cliente envia para o servidor uma mensagem de Accounting-Request, com opção STOP.
  - Ao receber esta msg, o servidor regista a data/hora de fim da sessão, e alguns parâmetros adicionais que tenham sido enviados pelo cliente (tempo, trafego, etc)
  - O servidor deve responder a este pedido com uma mensagem *Accounting-Response*

Acesso RADIUS



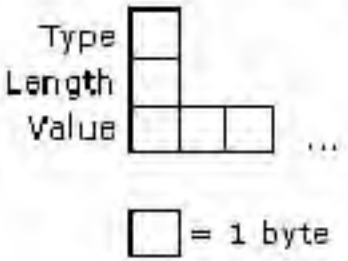
Nota: o protocolo inicial Access-Request/Access-Accept pode ser duplicado caso o protocolo de autenticação é *challenge/response*

Atributos de *accounting*

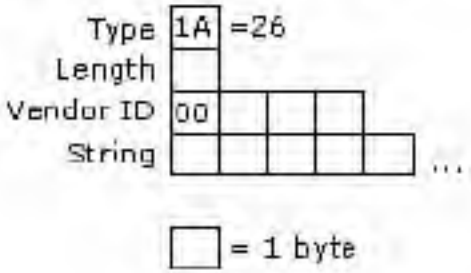
- As mensagens de *accounting* incluem geralmente listas de atributos que podem ser normalizadas ou específicas do fabricante
  - Neste último caso, o servidor de RADIUS dispõe normalmente de um dicionário de códigos de atributos que permite identificar os atributos e registá-los de forma legível

Atributos RADIUS

- Os atributos RADIUS são constituídos por um um tuplo (código, comprimento, valor). Uma mensagem pode incluir um ou mais atributos.



- Existe um código especial que permite aos fornecedores de equipamento incluirem informação adicional e específica do equipamento.



- O protocolo RADIUS é normalmente utilizado como suporte de autenticação na norma 802.1X
- O protocolo 802.1X permite que o acesso ao nível 2 da rede (em switchs ou pontos de acesso sem fios) só seja obtido após uma autenticação bem sucedida.
  ix No protocolo 802.1X são normalmente identificados três intervenientes
  - *Supplicant* - Terminal remoto que pretende acesso ao meio
  - *Authenticator* - Equipamento de rede que pretende autenticar o terminal remoto e que funciona como cliente do do servidor de autenticação.
  - *Authentication Server* - Servidor de autenticação (normalmente RADIUS)
- Antes do autenticador dar permitir acesso completo de nível 2 ao terminal, troca mensagens com este que são posteriormente encapsuladas no protocolo RADIUS
- Na fase de autenticação, o equipamento de rede limita-se a encapsular/desencapsular tramas que de facto têm origem e destino o terminal remoto.
- Quando a autenticação é bem sucedida, é o autenticador que recebe a mensagem de Access-Accept e viabiliza o acesso à rede.

802.1X e segurança

- Uma das caratcerísticas fundamentais do protocolo 802.1X é que a autenticação EAP circula de modo cifrado entre o terminal remoto e o servidor, sem intervenção do autenticador.
- Apesar do autenticador encapsular os pacotes EAP com RADIUS, não há qualquer informação que possa ser retirada relativa às credenciais do utilizador
- O mesmo sucede no caso de existirem sistema proxy de RADIUS de permeio. As mensagens são encaminhadas até ao servidor de destino sem qualquer e vice-versa sem quebra de confidencialidade nos nós intermédios.

RADIUS e 802.1X

Articulação entre os três intervenientes no processo de autenticação numa autenticação 802.1X com RADIUS. O servidor de autenticação pode ainda ser apenas um proxy-radius, caso em que realiza o *relay* das mensagens de autenticação para outro servidor.

Exemplos de registos RADIUS de *account*: START record. rede WiFi do IST

```
Tue Sep 27 14:20:02 2005
        Acct-Session-Id = "00002E77"
        Called-Station-Id = "000f.3446.8c60"
        Calling-Station-Id = "0011.2492.0af6"
        Cisco-AVPair = "ssid=e-U"
        Cisco-AVPair = "nas-location=unspecified"
        User-Name = "anonymousfcr"
        Acct-Status-Type = Start
        NAS-Port-Type = Wireless-802.11
        Cisco-NAS-Port = "11168"
        NAS-Port = 11168
        Service-Type = Framed-User
        NAS-IP-Address = 10.0.1.7
        Acct-Delay-Time = 0
        Client-IP-Address = 193.136.128.19
        Acct-Unique-Session-Id = "1375ba30ea90779b"
        Timestamp = 1127827202
```

Exemplos de registos RADIUS de *account*: STOP record, rede WiFi do IST

```
Tue Sep 27 14:34:31 2005
        Acct-Session-Id = "00002E77"
        Called-Station-Id = "000f.3446.8c60"
        Calling-Station-Id = "0011.2492.0af6"
        Cisco-AVPair = "ssid=e-U"
        Cisco-AVPair = "nas-location=unspecified"
        Cisco-AVPair = "vlan-id=230"
        Cisco-AVPair = "auth-algo-type=eap-peap"
        User-Name = "anonymousfcr"
        Cisco-AVPair = "connect-progress=Call Up"
        Acct-Session-Time = 868
        Acct-Input-Octets = 136092
        Acct-Output-Octets = 4103486
        Acct-Input-Packets = 1003
        Acct-Output-Packets = 3108
        Acct-Terminate-Cause = Lost-Carrier
        Cisco-AVPair = "disc-cause-ext=No Reason"
        Acct-Status-Type = Stop
        NAS-Port-Type = Wireless-802.11
```

```
Cisco-NAS-Port = "11168"
NAS-Port = 11168
Service-Type = Framed-User
NAS-IP-Address = 10.0.1.7
Acct-Delay-Time = 0
Client-IP-Address = 193.136.128.19
Acct-Unique-Session-Id = "1375ba30ea90779b"
Timestamp = 1127828071
```